IN THE UNITED STATES

PATENT AND TRADEMARK OFFICE

APPLICANTS:	Carey S. Nachenberg et al.
APPLICATION NO.:	10/046,496
FILING DATE:	October 29, 2001
TITLE:	Temporal Access Control for Computer Virus Outbreaks
EXAMINER:	Jeffery L. Williams
GROUP ART UNIT:	2137
ATTY. DKT. NO.:	20423-05957

CERTIFICATE OF ELECTRONIC (EFS-WEB) TRANSMISSION

I hereby certify that this correspondence is being transmitted via the Office electronic filing system in accordance with 37 C.F.R. § 1.8(a)(i)(C) from the Pacific Time Zone of the United States on the local date shown below.

Dated: _____ By: ___//_____

APPEAL BRIEF

Real Party in Interest

The subject application is owned by Symantec Corporation of Cupertino, California.

Related Appeals and Interferences

There are no known related appeals or interferences that may directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1-17, 20, and 22-34 are pending and stand rejected. The claims on appeal are claims 1-17, 20, and 22-34, which are set forth in the Claims Appendix.

Status of Amendments

Appellants have not amended the claims since the final rejection.

Summary of the Claimed Subject Matter

The claimed invention uses a virus outbreak report indicating a virus attack to compute a computer virus alert time (Specification, ¶¶ 38, 43, 69; Figure 4, 407). The computer virus alert time (Figure 2A, 204) is compared with a time stamp corresponding to an earliest moment or first time computer code was allowed to execute on a computer coupled to a computer network (Specification, ¶¶ 38, 78; Figure 4, 421), and the executability of the computer code is determined in response to the comparison (Specification ¶ 78; Figure 4, 421, 423, 425).

More specifically, claim 1 recites a computer-implemented method for computer virus prevention, said method comprising the steps of:

entering a first computer virus status mode in response to a first computer virus outbreak report indicating a virus attack threat to a computer network (Specification, ¶¶ 34, 67, 68; Figure 4, 403);

computing a first computer virus alert time corresponding to entry into the first computer virus status mode (Specification, ¶¶ 38, 69, 80; Figure 4, 407);

comparing a time stamp of executable computer code corresponding to an earliest moment the computer code was allowed to execute on a computer coupled to the computer network with the first computer virus alert time (Specification, ¶¶ 75, 78; Figure 4, 421); and

determining the executability of the computer code in response to the result of the comparing step (Specification, ¶¶ 75, 78; Figure 4, 421, 423, 425).

Claim 12 recites a computer access control system for computer virus prevention, said system comprising:

a computer configured to execute an access control console, for entering a first computer virus status mode in response to receiving a computer virus outbreak report indicating a virus attack threat to a computer network and for recovering a preselected virus access control time corresponding to said virus status mode (Specification, ¶¶ 34, 67, 68; Figure 1, 2, 3; Figure 2, 200); and

an anti-virus module, coupled to the access control console, configured to compute a virus alert time based on the virus access control time and to compare a time stamp of target executable computer code corresponding to an earliest moment the computer code was allowed to execute on a computer coupled to the computer network with the virus alert time prior to execution of the target executable computer code (Specification, ¶¶ 38, 69, 75, 78, 80; Figure 2, 200, 209), and

wherein the anti-virus module is further configured to determine whether to execute the target executable computer code in response to comparing the time stamp of the target executable computer code with the virus alert time (Specification, ¶¶ 75, 78).

Claim 20 recites a computer-implemented method for computer virus prevention, said method comprising the steps of:

creating a list of executable computer files, each file time-stamped with an execution time of the file, the execution time corresponding to an earliest moment the computer file was allowed to execute on a computer coupled to a computer network (Specification, ¶¶ 38, 57, 61; Figure 2, 205; Figure 3, 309);

entering a virus alert mode in response to a virus outbreak report indicating a virus attack threat to the computer network (Specification, ¶¶ 34, 67, 68; Figure 4, 403);

responsive to the virus alert mode, entering an access control message for specifying an access control rule for blocking the execution of suspicious or susceptible executable computer files that have a time stamp not before a computed virus alert time, the access control message including a first control parameter for computing the virus alert time (Specification, ¶¶ 35, 38, 69; Figure 2A, 202; Figure 4, 403);

receiving a request to execute a target executable computer file (Specification, ¶ 74; Figure 4, 409); and

determining whether to execute the target executable computer file based on the access control rule in the access control message (Specification, ¶¶ 75, 78; Figure 4, 421, 423, 425).

Claim 27 recites a computer-implemented method for computer virus prevention, said method comprising the steps of:

creating a list of executable computer files, each file time-stamped with an execution time of the file (Specification, ¶¶ 38, 57, 61; Figure 2A, 205; Figure 3, 309);

entering a virus alert mode in response to a virus outbreak report indicating a virus attack threat to a computer network (Specification, ¶¶ 34, 67, 68, 89; Figure 4, 403);

responsive to the virus alert mode, entering an access control message for specifying an access control rule for blocking data communication initiated by computer files that have a time stamp corresponding to an earliest moment the computer file was allowed to execute on a computer coupled to the computer network, and the time-stamp is not before a virus alert time, the access control message including a first control parameter for computing the virus alert time (Specification, ¶¶ 35, 38, 69, 89; Figure 4, 409; Figure 6, 200A, 202A);

receiving a request to examine a target executable computer file that participates in the data communication (Specification, ¶¶ 90, 91; Figure 7, 709); and

determining whether the data communication should be blocked based on the access control rule (Specification, ¶¶ 91, 92, 93; Figure 7, 719, 721, 723).

Claim 30 recites a computer program product comprising:

a computer usable storage medium having computer executable code embodied therein for computer access control for computer virus prevention, the computer program product comprising:

a firewall module monitoring data communications initiated by a target executable computer file and sending a request to examine the data communications (Specification, ¶¶ 88, 90, 91; Figure 6, 601);

an access control console, for generating an access control message specifying an access control rule for blocking data communications of the target executable computer file that has a time stamp corresponding to an earliest moment the computer file was allowed to execute on a computer coupled to a computer network, and the time-stamp is not before a virus alert time, the access control message including a first control parameter for computing the virus alert time in response to receiving a virus outbreak report indicating a virus attack threat to the computer network (Specification, ¶¶ 35, 38, 69, 89; Figure 2, 200; Figure 4, 409); and

an access control module, coupled to the access control console and the firewall module, configured to receive the access control message and a request from the firewall module, and to compute the virus alert time based on the virus access control time and to determine whether the data communication should be blocked based on the access control rule (Specification, ¶¶ 91, 92, 93; Figure 6, 203A).

Claim 31 recites a computer program product comprising:

a computer usable storage medium having computer executable code embodied therein for computer access control for computer virus prevention, the computer program product comprising:

a computer readable program code device configured to receive a computer virus status mode in response to a computer virus outbreak report indicating a virus attack threat to a computer network (Specification, ¶¶ 34, 67, 68; Figure 2, 203);

a computer readable program code device configured to compute a computer virus alert time corresponding to entry into the computer virus status mode (Specification, ¶¶ 38, 69, 80; Figure 2, 203);

a computer readable program code device configured to compare a time stamp of an executable computer file corresponding to an earliest moment the computer file was allowed to execute on a computer coupled to the computer network with the computer virus alert time (Specification, ¶¶ 75, 78; Figure 2, 203); and

a computer readable program code device configured to determine whether to execute the executable computer file in response to the result of comparing the time stamp of the computer content with the computer virus alert time (Specification, ¶¶ 75, 78; Figure 2, 203).

Claim 32 recites a computer program product comprising:

a computer usable storage medium having computer executable code embodied therein for computer access control for computer virus prevention, the computer program product comprising:

means for entering a computer virus status mode in response to receiving a virus outbreak report indicating a virus attack threat to a computer network and for generating a virus access control time (Specification, ¶¶ 34, 67, 68; Figure 2, 203);

coupled to the entering and generating means, means for computing a virus alert time based on the virus access control time (Specification, ¶¶ 38, 69, 80; Figure 2, 203); and

coupled to the computing virus alert time means, means for comparing a time stamp of a target executable computer file corresponding to an earliest moment the computer file was allowed to execute on a computer coupled to the computer network with the virus alert time prior to execution of the target executable computer file and for determining whether to execute the target executable computer file in response to comparing the time stamp of

the target executable computer file with the virus alert time (Specification, ¶¶ 75, 78; Figure 2, 203).

Claim 34 recites a computer-implemented method for computer virus prevention, said method comprising the steps of:

entering a first computer virus status mode in response to a first computer virus outbreak report indicating a virus attack threat to a computer network (Specification, ¶¶ 34, 67, 68; Figure 4, 403);

computing a first computer virus alert time corresponding to entry into the first computer virus status mode (Specification, ¶¶ 38, 69, 80; Figure 4, 407);

comparing a time stamp of executable computer code corresponding to a first time the computer code was allowed to execute on a computer coupled to the computer network with the first computer virus alert time (Specification, ¶¶ 75, 78; Figure 4, 421); and

determining the executability of the computer code in response to the result of the comparing step (Specification, ¶¶ 75, 78; Figure 4, 421, 423, 425).

Grounds of Rejection to be Reviewed on Appeal

The grounds of rejection presented for review in the present appeal are as follows:

1. Whether Bates et al., U.S. Patent 6,721,721 B1, in view of Hericourt et al., U.S. Patent 7,099,916, render claims 1-10 and 12-34 obvious under 35 U.S.C. § 103(a).

2. Whether Bates and Hericourt in view of Symantec, "Norton AntiVirus Corporate Edition," render claim 11 obvious under 35 U.S.C. § 103(a).

Argument

The claimed invention uses a virus outbreak report indicating a virus attack to compute a computer virus alert time. The computer virus alert time is compared with a time stamp corresponding to an earliest moment or first time computer code was allowed to execute on a computer coupled to a computer network, and the executability of the computer code is determined in response to the comparison. Specifically, independent claims 1, 12, 20, 27, 30, 31, 32 recite limitations similar to:

> entering a first computer virus status mode in response to a first computer virus outbreak report indicating a virus attack threat to a computer network;
> computing a first computer virus alert time corresponding to entry into the first computer virus status mode;
> *comparing a time stamp of executable computer code corresponding to an earliest moment the computer code was allowed to execute on a computer coupled to the computer network with the first computer virus alert time; and*
> determining the executability of the computer code in response to the result of the comparing step.

(quoting from claim 1). Dependent claim 8 further recites that the "computer code is determined to be executable only when the computer code is time stamped prior to the first computer virus alert time." In other words, the computer code is executable because it executed before the virus alert and, therefore, is unlikely to be infected by the virus implicated in the alert. Independent claim 34 resembles claim 1, except that the time stamp of the executable computer code corresponds "to a *first time* the computer code was allowed to execute on a computer coupled to the computer network."

The cited references, at the least, fail to disclose a time stamp "corresponding to an *earliest moment* the computer code was allowed to execute on a computer…" or "corresponding to a *first time* the computer code was allowed to execute on a computer…" Bates discloses a system that integrates virus checking functionality into a computer database search environment,

thereby allegedly decreasing the risks of viruses associated with accessing search results from computer database searches. *See* Bates, Abstract; column 3, lines 1-3. At col. 9, line 56 – col. 10, line 8, Bates describes how the user can assess the "trustworthiness" of a search result file by setting a virus criterion as to (i) whether the file has been virus checked within a predetermined period of time; (ii) whether the file has been changed since the last time a virus check was performed; or (iii) whether a particular period of time has elapsed in which the file has been found to be free of viral infection. Thus Bates at most discloses use of a single time stamp indicating the time the file was *last checked* for a virus. There is no teaching or suggestion in Bates of a time stamp that indicates the earliest moment or first time computer code was allowed to execute.

In fact, Bates does not even teach or suggest recording computer code execution times. The Examiner acknowledges this deficiency of Bates, and seeks to cure it by citing to Hericourt. This latter reference provides an overview of antivirus software, and describes how a suspect file can be executed in a protected location to see if it exhibits any virus-like behavior. Hericourt, col. 3, lines 52-54. Hericourt does not teach or suggest using time stamps for any purpose. However, the Examiner alleges that Hericourt teaches that scanning a file can comprise an execution of the file. Therefore, according to the Examiner, when Bates and Hericourt are combined Bates' time stamp indicating when a file was found free of a viral infection becomes a time stamp indicating when the file was executed.

The combination of Bates and Hericourt does not render the claimed invention obvious because neither reference discloses or suggests using a time stamp that corresponds to an earliest moment, or first time, the computer code was allowed to execute on a computer coupled to a computer network. If the references are combined in the manner suggested by the Examiner, the

time stamp at most represents a code execution occurring at an arbitrary time. The combination does not teach or suggest time stamping the earliest or first time code was executed; there might have been prior executions occurring before the time-stamped execution. Moreover, even if a particular time stamp in Bates did represent the earliest code execution, this happenstance event would not support the rejection. *See In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999) (stating that the mere fact that a certain thing may result from a given set of circumstances is not sufficient to support a rejection based on inherency); MPEP 2112 IV. Thus, a person of ordinary skill in the art at the time the invention was made, considering the teachings of the references either alone or in combination, would not find the claimed invention obvious.

The Examiner's defense of this rejection is essentially predicated on an unreasonable interpretation of the claims. Claims must be given their broadest reasonable interpretation consistent with the specification. *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005); MPEP § 2111. Here, the Examiner's interpretation is unreasonable because it calls code executions "earliest" or "first" even if prior code executions have occurred on a computer coupled to the network.

The unreasonableness of the Examiner's interpretation is demonstrated through Appellants' and the Examiner's exchanges concerning this rejection. In a previous Office Action, the Examiner supported the rejection by stating that code can be executed multiple times, and that:

> ...out of the multitude of instances a particular piece of computer code is executed, either via scanning or via end-user execution, the timestamp associated with the virus check for that computer code represents "an earliest execution time" in comparison to subsequent instances of execution for that piece of computer code.

(Office Action of January 11, 2008, page 18 lines 2-6). In response, Appellants argued that:

> a particular timestamp in Bates cannot be said to represent the "earliest" execution because there are an arbitrary number of executions that occur before and after the execution represented by the timestamp.

(Amendment of April 10, 2008, page 14 lines 18-21). Thus, Appellants argued that there can be any number of executions *before and after* a given execution, and no time stamp in Bates necessarily represents the earliest or first execution.

The Examiner now asserts that Appellants have "admitted" that the time stamped "'execution time' is subsequently followed by a plurality of executions of the software." (Office Action of July 10, 2008, page 4 lines 12-14). And, therefore, Appellants:

> reasonably must also acknowledge that within such a sequence the time-stamped execution represents "**an** earliest" time of execution in comparison to the subsequent executions within that sequence

(Office Action of July 10, 2008, page 17, lines 10-13, emphasis in original).

In other words, the Examiner calls any given time-stamped execution the "earliest" or "first" one by arbitrarily excluding from consideration any executions that came before it. For example, if there were three sequential executions, the Examiner would call execution two "an earliest" execution because it occurred before execution three, even though execution one occurred earlier. Moreover, if there were a sequence of 10 time stamps, the Examiner would call nine of the time stamps "first." This interpretation is improper because it is clearly unreasonable.

The Symantec reference fails to remedy the deficiencies of Bates and Hericourt described above. Therefore, a person of ordinary skill in the art, considering the teachings of the references either alone or in combination would not find the claimed invention obvious.

Based on the foregoing, Appellants submit that each of the pending rejections suffers from a clear deficiency in the *prima facie* case asserted in support of the rejection. Accordingly, Appellants request that the rejections of the claims be overturned.

Respectfully submitted,
CAREY S. NACHENBERG ET AL.

Dated: December 29, 2008

By: /Brian Hoffman/

Brian Hoffman, Reg. No. 39,713
Attorney for Assignee
Fenwick & West LLP
801 California Street
Mountain View, CA 94041
Tel.: (415) 875-2484
Fax: (415) 281-1350

Claims Appendix

1. A computer-implemented method for computer virus prevention, said method comprising the steps of:

entering a first computer virus status mode in response to a first computer virus outbreak report indicating a virus attack threat to a computer network;

computing a first computer virus alert time corresponding to entry into the first computer virus status mode;

comparing a time stamp of executable computer code corresponding to an earliest moment the computer code was allowed to execute on a computer coupled to the computer network with the first computer virus alert time; and

determining the executability of the computer code in response to the result of the comparing step.

2. The method of claim 1, wherein the step of computing the first virus alert time comprises the steps of:

receiving a first access control time based on the first virus outbreak report; and

converting the first access control time into the first virus alert time.

3. The method of claim 2, wherein the first access control time is a relative time stamp.

4. The method of claim 2, wherein the first access control time is a pre-determined time period for access control under the first computer virus status mode.

5. The method of claim 1, further comprising the step of:

determining the presence of a value representing the computer code in a memory table of executable computer content.

6. The method of claim 5, wherein the computer code is not executed when the value representing the computer code is not present in the memory table of executable computer code.

7. The method of claim 5, wherein the value is a hash value of the computer code.

8. The method of claim 1, wherein the computer code is determined to be executable only when the computer code is time stamped prior to the first computer virus alert time.

9. The method of claim 1, further comprising the steps of:

entering types of computer codes that should be blocked from execution in response to the first computer virus outbreak report; and

blocking execution of a computer code that belongs to the entered types of computer codes.

10. The method of claim 1, further comprising the steps of:

generating a second virus alert time in response to a second computer virus outbreak report;

comparing the time stamp of the computer code with the second computer virus alert time;

performing anti-virus processing upon the computer code; and

determining the executability of the computer code in response to the result of comparing the time stamp of the computer code with the second computer virus alert time.

11. The method of claim 1, wherein the computer code is attached to an E-mail body, and said method further comprises the steps of:

removing the computer code from the E-mail body; and

denying execution of the computer code.

12. A computer access control system for computer virus prevention, said system comprising:

a computer configured to execute an access control console, for entering a first computer virus status mode in response to receiving a computer virus outbreak report indicating a virus attack threat to a computer network and for recovering a preselected virus access control time corresponding to said virus status mode; and

an anti-virus module, coupled to the access control console, configured to compute a virus alert time based on the virus access control time and to compare a time stamp of target executable computer code corresponding to an earliest moment the computer code was allowed to execute on a computer coupled to the computer network with the virus alert time prior to execution of the target executable computer code, and

wherein the anti-virus module is further configured to determine whether to execute the target executable computer code in response to comparing the time stamp of the target executable computer code with the virus alert time.

13. The system of claim 12, wherein the target computer code is one of a plurality of computer code files, and the anti-virus module further comprises:

a memory module for storing time stamps of the plurality of computer code files; and

an access control module, coupled to the access control console and to the memory module, for computing the virus alert time and for comparing the time stamp of a target executable computer code with the virus alert time.

14. The system of claim 13, wherein the anti-virus module further comprises:

a computer virus processing module, coupled to the access control module, for further processing the target executable computer code in order to determine whether to execute the target executable computer code.

15. The system of claim 13, wherein the memory module stores a value representing each of the computer code files.

16. The system of claim 15, wherein the access control module is configured to determine the presence of the value in the memory module as representing a target executable computer code.

17. The system of claim 15, wherein the value is a hash value.

20. A computer-implemented method for computer virus prevention, said method comprising the steps of:

creating a list of executable computer files, each file time-stamped with an execution time of the file, the execution time corresponding to an earliest moment the computer file was allowed to execute on a computer coupled to a computer network;

entering a virus alert mode in response to a virus outbreak report indicating a virus attack threat to the computer network;

responsive to the virus alert mode, entering an access control message for specifying an access control rule for blocking the execution of suspicious or susceptible executable computer files that have a time stamp not before a computed virus alert time, the access control message including a first control parameter for computing the virus alert time;

receiving a request to execute a target executable computer file; and

determining whether to execute the target executable computer file based on the access control rule in the access control message.

22. The method of claim 20, wherein the step of determining whether to execute the target computer file comprises the steps of:

receiving the access control message;

automatically converting the first control parameter into the virus alert time;

comparing the time stamp of the target computer file in the list with the virus alert time; and

determining whether to execute the target executable computer file based on the result of the comparing step.

23. The method of claim 22, further comprising the step of:

applying an anti-virus operation upon the target executable computer file.

24. The method of claim 20, wherein the control message comprises:

a second control parameter for specifying types of computer files that should be subject to the access control rule;

a third control parameter for specifying an expiration time for the access control rule; and

a fourth control parameter for identifying the access control message.

25. The method of claim 24, further comprising the step of:

determining validity of the access control message based on the third control parameter.

26. The method of claim 24, further comprising the step of:

determining whether to execute the target executable computer file based on the second control parameter.

27. A computer-implemented method for computer virus prevention, said method comprising the steps of:

creating a list of executable computer files, each file time-stamped with an execution time of the file;

entering a virus alert mode in response to a virus outbreak report indicating a virus attack threat to a computer network;

responsive to the virus alert mode, entering an access control message for specifying an access control rule for blocking data communication initiated by computer

files that have a time stamp corresponding to an earliest moment the computer file was allowed to execute on a computer coupled to the computer network, and the time-stamp is not before a virus alert time, the access control message including a first control parameter for computing the virus alert time;

receiving a request to examine a target executable computer file that participates in the data communication; and

determining whether the data communication should be blocked based on the access control rule.

28. The method of claim 27, wherein the step of determining whether the data communication should be blocked comprises the steps of:

receiving the access control message;

converting the first control parameter into the virus alert time;

comparing the time stamp of the target executable computer file in the list with the virus alert time; and

determining whether the data communication should be blocked based on the comparing step.

29. The method of claim 28, wherein the data communication is blocked when the target executable computer file is time-stamped not before the virus alert time.

30. A computer program product comprising:

a computer usable storage medium having computer executable code embodied therein for computer access control for computer virus prevention, the computer program product comprising:

a firewall module monitoring data communications initiated by a target executable computer file and sending a request to examine the data communications;

an access control console, for generating an access control message specifying an access control rule for blocking data communications of the target executable computer file that has a time stamp corresponding to an earliest

moment the computer file was allowed to execute on a computer coupled to a computer network, and the time-stamp is not before a virus alert time, the access control message including a first control parameter for computing the virus alert time in response to receiving a virus outbreak report indicating a virus attack threat to the computer network; and

an access control module, coupled to the access control console and the firewall module, configured to receive the access control message and a request from the firewall module, and to compute the virus alert time based on the virus access control time and to determine whether the data communication should be blocked based on the access control rule.

31. A computer program product comprising:

a computer usable storage medium having computer executable code embodied therein for computer access control for computer virus prevention, the computer program product comprising:

a computer readable program code device configured to receive a computer virus status mode in response to a computer virus outbreak report indicating a virus attack threat to a computer network;

a computer readable program code device configured to compute a computer virus alert time corresponding to entry into the computer virus status mode;

a computer readable program code device configured to compare a time stamp of an executable computer file corresponding to an earliest moment the computer file was allowed to execute on a computer coupled to the computer network with the computer virus alert time; and

a computer readable program code device configured to determine whether to execute the executable computer file in response to the result of comparing the time stamp of the computer content with the computer virus alert time.

32. A computer program product comprising:

a computer usable storage medium having computer executable code embodied therein for computer access control for computer virus prevention, the computer program product comprising:

means for entering a computer virus status mode in response to receiving a virus outbreak report indicating a virus attack threat to a computer network and for generating a virus access control time;

coupled to the entering and generating means, means for computing a virus alert time based on the virus access control time; and

coupled to the computing virus alert time means, means for comparing a time stamp of a target executable computer file corresponding to an earliest moment the computer file was allowed to execute on a computer coupled to the computer network with the virus alert time prior to execution of the target executable computer file and for determining whether to execute the target executable computer file in response to comparing the time stamp of the target executable computer file with the virus alert time.

34. A computer-implemented method for computer virus prevention, said method comprising the steps of:

entering a first computer virus status mode in response to a first computer virus outbreak report indicating a virus attack threat to a computer network;

computing a first computer virus alert time corresponding to entry into the first computer virus status mode;

comparing a time stamp of executable computer code corresponding to a first time the computer code was allowed to execute on a computer coupled to the computer network with the first computer virus alert time; and

determining the executability of the computer code in response to the result of the comparing step.

Evidence Appendix

None

Related Proceedings Appendix

None